CVE-2023-0401

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-0401
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-08 20:15:00 UTC
Updated	2024-02-04 09:15:00 UTC
Description	A NULL pointer can be dereferenced when signatures are being verified on PKCS7 signed or signedAndEnveloped data. In

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	All	All	All	All
Application	Stormshield	Stormshield Management Center	All	All	All	All

References

Reference	Source	Link	Tags
www.openssl.org/news/secadv/20230207.txt	MISC	www.openssl.org	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
OpenSSL: Multiple Vulnerabilities (GLSA 202402-08) — Gentoo security		security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160481 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-0946)

160492 Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-12152)

183982 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2023-0401)

199150 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5844-1)

200021 Ubuntu Security Notification for Node.js Vulnerabilities (USN-6564-1)

241227 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:0946)

241256 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1199)

283694 Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2023-57f33242bc)

283736 Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2023-a5564c0a3f)

330133 IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory38)

355230 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-101

378491 NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Multiple OpenSSL Denial of Service (DoS) Vulnerabilities (NTAP-20230214-0011)

38894 Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities

502653 Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)

502757 Alpine Linux Security Update for openssl

691051 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (648a432c-a71f-11ed-86e9-d4c9ef517024)

710857 Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202402-08)

753640 SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2023:0312-1)

940941 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:0946)

960889 Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2023:0946)